TITLE OF INVENTION : IDENTITY SOFTWARE FOR RESTRICTING OTHER SOFTWARE SUPPLIED THROUGH A COMMUNICATION LINK OR THE LIKE TO BE USED ON ONE COMPUTER AND METHOD THEREFOR.

INVENTOR : HO KEUNG, TSE.

375-00-201-A

08/587448

A
B
B

~~Identity software~~ for restricting software ~~supplied through a communication link or the like~~ to be used ~~on one computer and method therefor~~

Field of the invention

The present invention relates to protection of commercial software sold through a communication link or the like, and particularly, to protection of such software against unauthorised use.

Background of the invention

Conventionally, software protection methods for protecting commercial software products such as programs, multimedium software, sold through a communication link, such as telephone line by means of modem, requires a user computer to install a hardware means which comprises, for instance, descryption keys and system therein for to be authenticated by a software running thereon. Hardware means, rather than software means, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a software means to replace the above-mentioned hardware means and which would not be copied by its rightful user to someone else.

It is therefore another object of the present invention to provide a method for detering unauthorised copying or use of the software means.

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a program for providing Encrypted Identity (hereinbelow referred as EI program), 2) a program for enabling software

(hereinbelow referred as ES program), 3) a program for authenticating computer (hereinbelow referred as AC program).

The central program is for managing the use of the individual programs therein so that the ES program can be protected from being accessed by the user directly, thereby preventing it to be copied individually. The EI program is for providing encrypted identity of a user for accessing a network central computer to obtain services or software products or alike inwhich a secure operation of a user account for payment therefor involved. The AC program is for authenticating the computer on which it runs by determining its hardware and software configuration by software means and comparing the result with that required. The ES program is for using the authentication result of the AC program ~~and the present of the EI program.~~ as a precondition for enabling those software obtained to run on a computer.

It should be noted that in the central program, the ES program is the one which needs protection most whereas the EI program needs least and according to the present invention, the ES program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a user would not copy a program (i.e., the EI program) which can provided the user's encrypted identity for using the user's account in obtaining, for eg., network services or software products to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily forged, has proved to be remarkedly secure.

According to a second embodiment of the present invention, the central program comprising only the EI program and the ES program enables software runs only when the EI program is present on the same computer which is determined by receiving an encrypted identity of the EI program from the same.

According to the third embodiment, the EI and ES programs are basically equivalent such that copying the ES program by its rightful user to someone else is equivalent to copying the EI program, thereby preventing the ES program from unauthorised copied or use.

Brief dscription of drawing

FIG.1 is a block diagram of central program.

FIG.2 is a diagrammatic view of a program inwhich a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

The present invention is directed to protecting software supplied through a communication link, and for the sake of simplicity, the following description is directed to protection of such software in a IBM PC computer. And, the present invention will be described under the following headings:

1) The Central Program.

2) The Program for providing Encrypted Identity (EI program).

3) The Program for enabling software (ES program).

4) The Program for authenticating computer (AC program).

5) Other Embodiments.

1) The Central Program.

According to the first embodiment, there is provided a central program which being an executable program and can be caused to execution by user by entering its filename in DOS environment or by a running program, refer to FIG.1 which is a block diagram of the central program.

When a user desires to access a network central computer through a communication link, the user has first to cause it to execute. It will request the user to enter a password which if coincidents with that required, it will send an identity of the user to the central computer.

This requirement of user password is necessary to prevent someone to access the central computer and use the account of the rightful user without his authorisation.

Then the central program causes the EI program to execute for providing an encrypted identity of the user, that encrypted identity will also be send to the central computer. The central computer will permit the access request from the user if the unencrypted and encrypted identities are consistent with each other.

When a running program desires to execute the ES program to enables its operation or it to continue to run, it first prepares an input parameter for indicating to the ES program such a request and stores the input parameter in a predetermined location in RAM, then through the use of a PC DOS service for that purpose, it causes the central program to be download from a permanent storage, eg. harddisk, of the computer to RAM and be executed. The central program will first access the input parameter in the predetermined location and from it the central program can determined that the running program requests for an enable signal from the ES program, and will then cause the ES program to execute.

For the case the central program is caused by user to be executed, there will be no or no valid input parameter and the control program can thus know this fact.

2) The Program for providing Encrypted Identity (EI program).

This program borrows the technique used in IC credit card inwhich an encrypted identity is generated for identity authentication.

When starts, the EI program sends a access request to a central computer which in return will send back a random number. The EI program then encrypts the random number with a predetermined algorithm A1 and sends the result to the central computer which will permit access if the result is identical with the result it obtained by performing the same encryption.

It should be noted that for each user, there is a corresponding respective encryption algorithm A1 for identification of each of them and also that the central computer may use the encryption result, if it being correct, from the EI program as a

user authorisation for payment to be made, from a user account for obtaining network services or software products or the like.

3) The Program for enabling software (ES program).

According to the present invention, there are 2 approaches for enabling software :

i) by sending encrypted command to a running software for enabling operation of the same on the computer ~~by the technique as mentioned in item 2~~. Specifically, the running software includes in the input parameter, as mentioned above in item 1, a random number it generated, The ES program, in return sends the result it obtained by performing a predetermined encryption algorithm A2 on that random number, to the running software which will compare it with the result it obtained by performing the same encryption.

It should be noted that for each user, ~~each one of~~ the software for use on his/her computer(s) use a same respective encryption algorithm A2 and the encryption algorithm A2 being included into ~~each such one~~ by the central computer at the time when the central computer is to supply the same to the user computer.

ii) by descrypting a encrypted part of a software or an encrypted software.

It should be noted that if the software is a program, then it will be sufficient to have a part thereof to be encrypted, for preventing unauthorised copy and use, however, if the software is an audio/visual multimedium data file, it will be more desirable to have the whole software be encrypted.

The ~~description~~ of a part of or an entire software takes place on a temporary copy of which in RAM. Given by example only, FIG. 2 is a diagrammatic view of a program in RAM space, with a part B thereof being encrypted. As seen, the ES program descrypts part b and stores the result which size should be not equivalent to that of the encrypted origin in 'part B descrypted'.

~~. The ES program then overwrites at the first location of 'part B encrypted' an~~ instruction 'JUMP TO part B descrypted' and at the end of 'part B descrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and its descrypted part will be executed instead.

In the case of audio/visual multimedium software, the software will be descrypted a small part by a small part and each small part is descrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the ES program to be executed in the manner as described above in item 1, everytime it wants a descryption of a small part. Desirable, a newly descrypted small part will overwrite a previous descrypted one so that a whole copy of the descrypted software will not exist in RAM.

4) The Program for authenticating computer (AC program).

One object of this program is to prevent the central program from being used , if it is a copy being made by someone other than the rightful user and of this the rightful user being unawared, so that a rightful user need not guard his computer containing the central program from reach of someone else.

When the central program is installed in a harddisk of a user computer and executed, it will check a encrypted status information in it and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to a central computer an unencrypted identity of the user, then the AC program requests for a encrypted command from a central computer which will provide such a encrypted command, in the manner as described hereinabove in item 3i, if the user has a valid account or the account is not closed.

After authenticating the command, the AC program determines the hardware and software configuration of the user computer, which includes, for eg., running ~~speed determination which is a function of CPU frequency, cache memory size etc;~~

number and identities of peripherals such as mouse, printer, joystick, harddisk and floppy disk drive etc; characteristic of hardware such as number of heads, cylinders, sectors of harddisk and locations of bad sectors therein; version number of operation system software and physical position of a particular software including the central program in the harddisk; by skills well known to those in the art. For instance, the running speed can be determined by and causing the computer to execute a test program and initializing a hardware counter to measure the time the computer has taken to finish the program. For another instance, the version number of the operation system may be determined by using a particular DOS service.

The result of the determination and a status information of being initialized is being stored by the AC program in a predetermined part of the central program in the form of encrypted data. Thereafter, everytime when the central program is executed, it will first check the status information, and after confirming that it is being initialized, it will perform a job as requested, referred to item 1, and in addition thereto, it will also automatically cause the AC program to execute which will determines at least a part of the above hardware and software configuration of the computer, at a time, and the AC program will encrypt an indication in another predetermined part of the central program for causing the ES program not to operate, if any of the configuration determined is not identical to that it encrypted and stored previously.

In addition thereto, the AC program will also reset the encrypted status information so that another initialization process will automatically take place if the user causes the central program to be executed, for which another encrypted command from the central computer will be required..

This prevents a user deliberately adapts the program to other user's computer, after closing his account.

In addition, the encrypted command from the central computer may be alternatively be supplied to the user via, eg., telephone line, and being enterred into the user computer by the user. Specifically, to request for a encrypted command, the AC

program generates a random number and displays the random number which is being supplied to the central computer by the user by means of telephone dual tone signals, generated by entering the random number on a telephone keypad, through telephone lines, and after encrypting the random number, the central computer sends the result to the user via the same telephone line by means of a voice synthesizer.

5) Other Embodiments

According to the second embodiment, the ES program is separate from the central program which comprises the EI and AC program. The ES program is bound with the EI program by requiring the ES program to operate only when the EI program is present on the same computer. Specifically, the ES program when running, can cause the EI program to be executed for generating an encrypted identity for the ES program to authenticate. The EI program knows that this is a request for encrypted identity from the ES program, not a request from user for encrypted identity for accessing a central computer, by the technique of input parameter as mentioned above in claim 1.

Further, the EI program before sending the encrypted identity to the ES program, may first check the data integrity of itself by, for instance, checksum method. Alternatively, it may also be that the ES program performs the checking. And, if the checking result is that some data in the EI program being altered, then ~~Then~~, in the former case, the ES will be caused to not operable by the EI program by not sending it a encrypted identity, and in the latter case, the ES program will be caused to not operable by itself.

According to the third embodiment, the encryption algorithms A1 and A2 that the EI and ES programs use respectively for providing encrypted identity to the central computer and for generating encrypted commands to enable running software respectively, is a same algorithm.

Thus, it would be equivalent for a rightful user to copy his EI program to someone else if he copies his ES program to someone else. In this case, a slight

modification on the ES program can make it operate in the same manner as the EI program, which involves adding a simply interface program for receiving a random number from a central computer, feeding the random number into the ES program, receiving the encrytion result from the ES program and supplying the encrytion result to the central computer, and such functions are commonly found in any network interface software.

In addition, according to another embodiment of the present invention, the software and ES program for use on a particular user's computer includes an identity of its rightful user, so as for facilitates legal action against piracy. Further, the ES program accesses software, by using a particular DOS service for loading a program from harddisk to RAM, stored in the computer onwhich it runs for such an identity therein, if any software is found to have an identity not identical to that of the ES program, the ES program will inhibit use of all software under its control, including itself, on the computer. Such identities may be stored in a predetermined location of the software, and is protected from being altered by having an encrypted one stored in another location in each software, and said another location differs to each another in different software so that it would not discovered and altered. And, each such software, when executed, will automatically check the unencrypted identity stored therein against the encrypted one, if they are not identical, the software will fail to operate. The identity or encrypted identity of the rightful user being included into each one of the software by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the ES program to mistakenly regard a software which stored in the computer and which being not supplied from the central computer, be a software under its control, the central may include a information in a predetermined location of the software for indicating this fact to the ES program and each one of the software will not operate if when being executed, it finds the information therein being altered.